

What is claimed is:

1. A maintenance interface user authentication apparatus in a client/server type distribution system having a plurality of client devices connected to a server device over a network,

said server device having:

a request receiving section which receives from a server-side console a user authentication information setting request including user authentication information and designation of said client devices and a nullification-of-user-authentication-information-setting request including designation of said client devices; and

a request transfer section which transfers said user authentication information setting request and said nullification-of-user-authentication-information-setting request, received by said request receiving section, to those of said client devices which are designated over said network,

each of said client devices having:

a user authentication section which authenticates a user at a time of using a maintenance interface; and

a remote request processing section which sets said user authentication information, included in said user authentication information setting request, in said user authentication section when receiving said user authentication information setting request from said server device over said network, and nullifies said user authentication information set in said user authentication

section when receiving said nullification-of-user-authentication-information-setting request from said server device over said network.

2. The maintenance interface user authentication apparatus according to claim 1, wherein setting of said user authentication information in said user authentication section in each of said client devices can be done only from said server-side console.

3. The maintenance interface user authentication apparatus according to claim 1, wherein said server device has an encryption section which encrypts said user authentication information in said user authentication information setting request to be transferred by said request transfer section, and each of said client devices has a decryption section which decrypts encrypted user authentication information in said user authentication information setting request received by said remote request processing section.

4. The maintenance interface user authentication apparatus according to claim 1, wherein each of said client devices has a cutoff enforcement section which forcibly disables use of a user who is currently using said maintenance interface in case where that user authentication information which is already set in said user authentication section is set again by a new user authentication information setting request received over said network.

5. The maintenance interface user authentication

apparatus according to claim 1, wherein each of said client devices has a use time management section which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable use time has elapsed since setting of said user authentication information in said user authentication section.

6. The maintenance interface user authentication apparatus according to claim 5, wherein each of said client devices has a use time extending section which extends a remaining use time of said use time management section by a predetermined extension time only for first log-in since opening of said maintenance interface.

7. The maintenance interface user authentication apparatus according to claim 6, wherein at a time a first log-in request is issued since opening of said maintenance interface, said use time extending section determines whether or not a remaining use time managed by said use time management section lies within a predetermined given time and extends said remaining use time of said use time management section by a predetermined extension time when said remaining use time lies within said predetermined given time.

8. The maintenance interface user authentication apparatus according to claim 6, wherein during first log-in since opening of said maintenance interface, said use time extending section determines whether or not a

remaining use time managed by said use time management section has fallen within a predetermined given time and extends said remaining use time of said use time management section by a predetermined extension time when  
5 said remaining use time has fallen within said predetermined given time.

9. The maintenance interface user authentication apparatus according to claim 5, wherein said use time management section uses, as said allowable use time, an  
10 allowable use time designated in said user authentication information setting request sent from said server device.

10. The maintenance interface user authentication apparatus according to claim 5, wherein said use time management section uses an allowable use time reference  
15 value prestored in said client devices as said allowable use time.

11. The maintenance interface user authentication apparatus according to claim 5, wherein when an allowable use time is designated in said user authentication  
20 information setting request sent from said server device, said use time management section uses said designated allowable use time as said allowable use time, and when said allowable use time is not designated, said use time management section uses an allowable use time reference  
25 value prestored in said client devices as said allowable use time.

12. The maintenance interface user authentication apparatus according to claim 1, wherein each of said

client devices has a log-in number management section which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable number of log-in events has taken place since setting of said user authentication information in said user authentication section.

13. The maintenance interface user authentication apparatus according to claim 9, wherein said log-in number management section uses, as said allowable number of log-in events, an allowable number of log-in events designated in said user authentication information setting request sent from said server device.

14. The maintenance interface user authentication apparatus according to claim 13, wherein said log-in number management section uses an allowable-number-of-log-in reference value prestored in said client devices as said allowable number of log-in events.

15. The maintenance interface user authentication apparatus according to claim 13, wherein when an allowable number of log-in events is designated in said user authentication information setting request sent from said server device, said log-in number management section uses said designated allowable number of log-in events as said allowable number of log-in events, and when said allowable number of log-in events is not designated, said log-in number management section uses an allowable-number-of-log-in reference value prestored in said client devices as

said allowable number of log-in events.

16. The maintenance interface user authentication apparatus according to claim 1, wherein each of said client devices has an authentication nullification section  
5 which nullifies said user authentication information set in said user authentication section at a time a user of said maintenance interface ends use of said maintenance interface.

17. A maintenance interface user authentication  
10 method in a client/server type distribution system comprising:

(a) a step in which a server device receives a user authentication information setting request including user authentication information and designation of client  
15 devices from a server-side console and transfers said user authentication information setting request to said designated client devices over a network;

(b) a step in which said client devices receive said user authentication information setting request over said  
20 network and set said user authentication information setting request in a user authentication section which authenticates a user at a time of using a maintenance interface;

(c) a step in which said server device receives a  
25 nullification-of-user-authentication-information-setting request including designation of said client devices from said server-side console and transfers said nullification-of-user-authentication-information-setting request to said

designated client devices over said network; and

(d) a step in which said client devices receive said nullification-of-user-authentication-information-setting request over said network and nullify said user authentication information set in said user authentication section.

18. The maintenance interface user authentication method according to claim 17, wherein setting of said user authentication information in said user authentication section in each of said client devices can be done only from said server-side console.

19. The maintenance interface user authentication method according to claim 17, wherein said step (a) includes a process of causing said server device to encrypt said user authentication information to be transferred and said step (b) includes a process of causing said client devices to decrypt said received user authentication information.

20. The maintenance interface user authentication method according to claim 17, wherein said step (b) includes a process of forcibly disabling use of a user who is currently using said maintenance interface in case where that user authentication information which is already set in said user authentication section is set again to new user authentication information received.

21. The maintenance interface user authentication method according to claim 17, further including:

(e) a step in which each of said client devices

nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable use time has elapsed since setting of said user authentication information in said user authentication section.

22. The maintenance interface user authentication method according to claim 21, further including:

(f) a step in which said each of said client devices extends a remaining use time of said use time management section by a predetermined extension time only for first log-in since opening of said maintenance interface.

23. The maintenance interface user authentication method according to claim 22, wherein at a time a first log-in request is issued since opening of said maintenance interface, said step (f) determines whether or not a remaining use time managed in said step (e) lies within a predetermined given time and extends said remaining use time by a predetermined extension time when said remaining use time lies within said predetermined given time.

24. The maintenance interface user authentication method according to claim 22, wherein during first log-in since opening of said maintenance interface, said step (f) determines whether or not a remaining use time managed in said step (e) has fallen within a predetermined given time and extends said remaining use time by a predetermined extension time when said remaining use time has fallen within said predetermined given time.



25. The maintenance interface user authentication method according to claim 21, wherein as said allowable use time in said step (e), an allowable use time designated in said user authentication information setting request sent from said server device is used.

26. The maintenance interface user authentication method according to claim 21, wherein as said allowable use time in said step (e), an allowable use time reference value prestored in said client devices is used.

27. The maintenance interface user authentication method according to claim 21, wherein when an allowable use time is designated in said user authentication information setting request sent from said server device, said designated allowable use time is used as said allowable use time in said step (e), and when said allowable use time is not designated, an allowable use time reference value prestored in said client devices is used as said allowable use time.

28. The maintenance interface user authentication method according to claim 17, further including:

(e) a step in which each of said client devices nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable number of log-in events has taken place since setting of said user authentication information in said user authentication section.

29. The maintenance interface user authentication

method according to claim 28, wherein as said allowable number of log-in events in said step (e), an allowable number of log-in events designated in said user authentication information setting request sent from said server device is used.

30. The maintenance interface user authentication method according to claim 29, wherein as said allowable number of log-in events in said step (e), an allowable-number-of-log-in reference value prestored in said client devices is used.

31. The maintenance interface user authentication method according to claim 29, wherein when an allowable number of log-in events is designated in said user authentication information setting request sent from said server device, said designated allowable number of log-in events is used as said allowable number of log-in events in said step (e), and when said allowable number of log-in events is not designated, an allowable-number-of-log-in reference value prestored in said client devices is used as said allowable number of log-in events.

32. The maintenance interface user authentication method according to claim 17, further including:

(e) a step in which each of said client devices nullifies said user authentication information set in said user authentication section at a time a user of said maintenance interface ends use of said maintenance interface.

33. A server device to be connected to a plurality

of client devices over a network, comprising:

5 a request receiving section which receives from a server-side console a user authentication information setting request including user authentication information, which is set in user authentication section for authenticating a user at a time said client devices use a maintenance interface, and designation of said client devices and a nullification-of-user-authentication-information-setting request including designation of said  
10 client devices; and

a request transfer section which transfers said user authentication information setting request and said nullification-of-user-authentication-information-setting request, received by said request receiving section, to  
15 those of said client devices which are designated over said network.

34. The server device according to claim 33, further having an encryption section which encrypts said user authentication information in said user authentication  
20 information setting request to be transferred by said request transfer section.

35. The server device according to claim 33, wherein each of said client devices has a structure for transmitting said allowable use time to be set in use time  
25 management section, which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an

allowable use time has elapsed since setting of said user authentication information in said user authentication section, in such a way as to be included in said user authentication information setting request.

5           36. The server device according to claim 33, wherein each of said client devices has a structure for transmitting said allowable number of log-in events to be set in a log-in number management section, which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user  
10           who is currently using said maintenance interface when an allowable number of log-in events has taken place since setting of said user authentication information in said user authentication section, in such a way as to be  
15           included in said user authentication information setting request.

37. A client device to be connected to a server device over a network, comprising:

20           a user authentication section which authenticates a user at a time of using a maintenance interface; and  
            a remote request processing section which sets user authentication information, included in a user authentication information setting request, in said user authentication section when receiving said user  
25           authentication information setting request including said user authentication information from said server device over said network, and nullifies said user authentication information set in said user authentication section when

receiving said nullification-of-user-authentication-information-setting request from said server device over said network.

38. The client device according to claim 37, wherein  
5 setting of said user authentication information in said user authentication section can be done only by said user authentication information setting request received from said server device.

39. The client device according to claim 37, further  
10 comprising a decryption section which decrypts encrypted user authentication information in said user authentication information setting request received from said server device over said network.

40. The client device according to claim 37, further  
15 comprising a cutoff enforcement section which forcibly disables use of a user who is currently using said maintenance interface in case where that user authentication information which is already set in said user authentication section is set again by a new user  
20 authentication information setting request received over said network.

41. The client device according to claim 37, further  
comprising a use time management section which nullifies  
said user authentication information set in said user  
25 authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable use time has elapsed since setting of said user authentication information in said user authentication

section.

42. The client device according to claim 41, further comprising a use time extending section which extends a remaining use time of said use time management section by  
5 a predetermined extension time only for first log-in since opening of said maintenance interface.

43. The client device according to claim 37, further comprising a log-in number management section which nullifies said user authentication information set in said  
10 user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable number of log-in events has taken place since setting of said user authentication information in said user authentication section.

15 44. The client device according to claim 37, further comprising an authentication nullification section which nullifies said user authentication information set in said user authentication section at a time a user of said maintenance interface ends use of said maintenance  
20 interface.

45. A server program for causing a computer constituting a server device to be connected to a plurality of client devices over a network to function as:  
a request receiving section which receives from a  
25 server-side console a user authentication information setting request including user authentication information, which is set in user authentication section for authenticating a user at a time said client devices use a

maintenance interface, and designation of said client devices and a nullification-of-user-authentication-information-setting request including designation of said client devices; and

5           a request transfer section which transfers said user authentication information setting request and said nullification-of-user-authentication-information-setting request, received by said request receiving section, to those of said client devices which are designated over  
10   said network.

46. The server program according to claim 45, wherein said computer is further caused to function as an encryption section which encrypts said user authentication information in said user authentication information  
15   setting request to be transferred by said request transfer section.

47. The server program according to claim 45, wherein said request receiving section and said request transfer section receive from said server-side console  
20   said allowable use time to be set in a use time management section, which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable use time has  
25   elapsed since setting of said user authentication information in said user authentication section, and transfer said allowable use time in such a way as to be included in said user authentication information setting

request.

48. The server program according to claim 45,  
wherein said request receiving section and said request  
transfer section receive from said server-side console  
5 section said allowable number of log-in events to be set  
in log-in number management section, which nullifies said  
user authentication information set in said user  
authentication section and forcibly disables use of a user  
who is currently using said maintenance interface when an  
10 allowable number of log-in events has taken place since  
setting of said user authentication information in said  
user authentication section, and transfer said allowable  
number of log-in events in such a way as to be included in  
said user authentication information setting request.

15 49. A client program for causing a computer  
constituting a client device to be connected to a server  
device over a network to function as:

a user authentication section which authenticates a  
user at a time of using a maintenance interface; and

20 a remote request processing section which sets user  
authentication information, included in a user  
authentication information setting request, in said user  
authentication section when receiving said user  
authentication information setting request including said  
25 user authentication information from said server device  
over said network, and nullifies said user authentication  
information set in said user authentication section when  
receiving said nullification-of-user-authentication-



information-setting request from said server device over said network.

50. The client program according to claim 49,  
wherein setting of said user authentication information in  
5 said user authentication section can be done only by said  
user authentication information setting request received  
from said server device.

51. The client program according to claim 49,  
wherein said computer is further caused to function as a  
10 decryption section which decrypts encrypted user  
authentication information in said user authentication  
information setting request received from said server  
device over said network.

52. The client program according to claim 49,  
15 wherein said computer is further caused to function as a  
cutoff enforcement section which forcibly disables use of  
a user who is currently using said maintenance interface  
in case where that user authentication information which  
is already set in said user authentication section is set  
20 again by a new user authentication information setting  
request received over said network.

53. The client program according to claim 49,  
wherein said computer is further caused to function as a  
use time management section which nullifies said user  
25 authentication information set in said user authentication  
section and forcibly disables use of a user who is  
currently using said maintenance interface when an  
allowable use time has elapsed since setting of said user

authentication information in said user authentication section.

54. The client program according to claim 53,  
wherein said computer is further caused to function as a  
5 use time extending section which extends a remaining use  
time of said use time management section by a  
predetermined extension time only for first log-in since  
opening of said maintenance interface.

55. The client program according to claim 49,  
10 wherein said computer is further caused to function as a  
log-in number management section which nullifies said user  
authentication information set in said user authentication  
section and forcibly disables use of a user who is  
currently using said maintenance interface when an  
15 allowable number of log-in events has taken place since  
setting of said user authentication information in said  
user authentication section.

56. The client program according to claim 49,  
wherein said computer is further caused to function as an  
20 authentication nullification section which nullifies said  
user authentication information set in said user  
authentication section at a time a user of said  
maintenance interface ends use of said maintenance  
interface.